EXHIBIT "F"

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ELISA BROOKS-CUNNINGHAM & COURTNEY DOUGLAS, *On behalf themselves and those similarly Situated*	) Case No.: 12-1524
Plaintiffs,	)
vs.	)
CONVERGENT OUTSOURCING, f/b/a ERS SOLUTIONS, INC	)
Defendant	)

DECLARATION OF EVAN HENDRICKS

1. I make this declaration as an expert in the field of information-privacy and principles of Fair Information Practices as it pertains to debt collection. (See attached CV, and section on "Qualifications & Background," below.)

2. I have been retained by Plaintiffs' counsel to provide expert opinion testimony on whether Defendant's letter to Plaintiffs revealed sensitive personal information and therefore violated Plaintiffs' privacy and triggered concerns about identity theft.

Legal Foundation

3. Section 1692f(8) of the Fair Debt Collection Practices Act (FDCPA) prohibits debt collectors such as Defendants from "Using any language or symbol, other than the debt collector's address, on any envelope when communicating with a consumer by use of the mails or by telegram, except that a debt collector may use his business name if such name does not indicate that he is in the debt collection business."

4. Defendant's envelope at issue in this case included a "QR Code" that revealed Plaintiffs' name, address, account number and amount allegedly owed. It is undisputed that the QR Code can be deciphered with an iPhone.

5. As part of its justification for including the QR Code symbol on the envelope, Defendant asserted that the information it revealed was "benign" or "innocuous language."

6. This is plainly wrong, as the QR Code revealed Plaintiffs' name, address, account number and amount allegedly owed. As I will detail below, such information clearly constitutes "sensitive information" under every known privacy standard and definition.

Sensitive Personal Information & Privacy

7. Privacy encompasses the right of individuals to maintain reasonable control over their personal information. In fact, Supreme Court Justice John Paul Stevens wrote, "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[1]

8. There are several landmark state and federal privacy laws -- all of which were enacted long before Defendant sent the envelope at issue in this case. All of these laws have definitions or standards that encompass the kind of personal information regarding Plaintiffs captured by Defendant's QR Code. These laws broadly define personal information to ensure maximum protection with two fundamental goals in mind: (1) the protection of personal privacy and (2) the prevention and/or mitigation of identity theft.

9. For instance, California's breach notification law, which spawned similar laws by the vast majority of states, defined "Personal information" broadly to ensure maximum protection. To wit:

> ...any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information ... (Calif. Civil Code, Section 1798.80-1798.84; www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84)

10. Congress enacted the Gramm-Leach-Bliley Act's (GLB) privacy provisions specifically to protect financial account information. It also defined "Nonpublic personal information" (NPI) broadly to ensure maximum protection. To wit:

> (A) ... [NPI] means personally identifiable financial information -
> (i) provided by a consumer to a financial institution;
> (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
> (iii) otherwise obtained by the financial institution ...

[1] U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989)

(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. (15 USC, Subchapter I, Sec. 6801-6809) www.ftc.gov/privacy/glbact/glbsub1.htm#6809

11. In 2003, Congress amended the Fair Credit Reporting Act (FCRA) to significantly strengthen privacy and security for credit and debit card account numbers by requiring merchants to truncate them so they would no longer be revealed on receipts. [15 U.S.C. § 1681c(g)(1)]

12. In 2010, the Federal Trade Commission, which not only oversees the FCRA, but also is considered the leading federal agency on consumer protection and privacy, issued its seminal report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." In that report, it defined "sensitive data" as those regarding health, *finances*, or children [emphasis added], adding, "Consumers may feel harmed when their personal information – particularly sensitive health or financial information – is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations." www.ftc.gov/os/2010/12/101201privacyreport.pdf

13. Clearly, Defendant's QR Code exposed sensitive information regarding Plaintiffs' finances, and did so without their "knowledge or consent [and] in a manner that is contrary to their expectations."

14. The grave importance of protecting sensitive information is underscored by the fact that since 2001, the FTC has brought twenty-three actions against companies that allegedly failed to provide reasonable protections for sensitive consumer information in both online and offline settings.[2]

---

[2] *See FTC v. Navone*, No. 2:08-CV-01842 (D. Nev. filed Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Genica Corp.*, FTC Matter No. 082-3133 (Feb. 5, 2009) (proposed consent agreement); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129

Identity Theft: Long-Standing, Well-Known Phenomenon

15. With an estimated 8-9 million victims per year for the past several years, it is undisputed that identity theft is a long-standing, well-known phenomenon.

16. One reason for its prevalence is that given the relatively easy availability of personal information that can be exploited, it is considered to many criminals as potentially a low-risk, high-reward crime.

17. Identity thieves come in many versions. Some have demonstrated persistence and industriousness. Some specialize in hacking servers and databases. Others prefer to exploit a position inside a major organization so as to filch personal data.

18. Possibly most relevant to this case is the prevalence of identity thieves who are members of meth-amphetamine gangs ("tweakers"), and who specialize in stealing mail so as to obtain exploitable personal information. Because of their direct threat to U.S. mail, these gangs have become the targets of U.S. Postal Inspectors (USPIS). USPIS inspectors have investigated and reported on the persistence and ingenuity of tweakers in finding ways to obtain exploitable personal information from mail pieces.[3]

19. Thus, exposing a consumer's sensitive information, as Defendant did in Plaintiffs' case, creates a real risk of identity theft.

20. Accordingly, it is specious for Defendant to assert that exposing the QR code in Plaintiffs' cases "doesn't mean anything," or "I don't think there's anything there." [Hunter Depo., pgs. 48-49].

21. It is important to note that QR Codes are distinct from the mail-delivery-related bar codes used by the U.S. Postal Service and major mailers.

22. It is also important to note consumers increasingly are using their smartphones applications to scan bar codes, as they can be used to find more information about products, watch videos, shop an m-commerce site, enter contests, and compare prices. More than 15 million consumers have used the ScanLife app. (www.internetretailer.com/2012/02/01/bar-code-scanning-goes-through-roof).

23. According to Scanbuy, a QR code provider of "of mobile barcode solutions that use the camera phone to connect the physical and digital world," the number of consumers

---

(Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[3] See, for example, "Meth Users, Attuned to Detail, Add Another Habit: ID Theft," July 11, 2006 www.nytimes.com/2006/07/11/us/11meth.html?pagewanted=all&_r=0

scanning bar codes through ScanLife jumped 206% in Q1 2012 to 5.2 million from 1.7 million in Q1 2011. (www.internetretailer.com/2012/05/17/scanlife-bar-code-scans-increase-160-q1-2012)

Defendant's Position Reflect Continuing Disregard

24. Defendant's argument that it was not wrong to expose the QR code, or that "the information revealed when the QR Code is scanned "doesn't mean anything," reflects a troubling disregard for well-known, long-standing standards of privacy and data security. As noted above, the QR Code reveals Plaintiff's name, address, account number and amount allegedly owed – placing it squarely in the category of sensitive personal information under widely accepted standards.

25. Also troubling is Defendant's lack of attention to the personal information exposed by its placement of the QR Code in plain sight, and its lack of concern for the potential damage to a consumer's privacy and security.

26. Given the importance of protecting privacy, and the fact that identity theft, stemming from mail theft, was a well-known, long-standing phenomenon, it was reckless for Defendant to have placed the QR Code – and the discoverable sensitive personal information it contained – in plain sight.

Materials Reviewed

27. I have reviewed the Amended Complaint and Second Amended Complaint, the depositions of ER Solutions, Inc. Robert Hunter and Anne Carlson, Defendant's Answer, Affirmative Defenses, and Demand for Jury.

Background & Qualifications

28. Since 1977, credit reporting issues, and the Federal and State laws governing them, have been an integral part of my professional life as an editor and publisher of a specialized newsletter, and for the past decade as an expert witness appearing before courts and Congress, and as an expert consultant to governmental, corporate and non-profit organizations. This is because the principles underlying the Federal Fair Credit Reporting Act (FCRA) are consistent with the "Fair Information Practices" principles (FIPs) that are at the core of most information-privacy laws. In fact, the FCRA (1970) was the first U.S. information-privacy law, preceding the Privacy Act of 1974, which governs federal agencies use of personal data.[4] A primary goal of the FIPs and the FCRA is to ensure that people are treated equitably and fairly when information about them from a third-party record serves as the basis for an organizational decision about them. FIPs and the FCRA attain this goal by creating *rights* for individuals in relation to information about them held by third parties, and by imposing *obligations*

[4] Fair Information Practices principles, and their link to the FCRA, Privacy Act, and numerous other national and foreign privacy laws, is explained in Personal Privacy In The Information Age: The Report of the Privacy Protection Study Commission, *(July 1977; GPO Stock No. 052-003-00395)*

on those third parties in regards to the collection, use, maintenance and disclosure of personal information. FIPs and FCRA recognize that ensuring privacy, defined as individuals maintaining reasonable control over their personal information,[5] has value, and that depriving people of such control, (invading privacy) is damaging.

29. My expertise in credit reporting stems from several of my professional activities, including: (1) Editor/Publisher of a specialty news reporting service that covers credit reporting; (2) author of the book Credit Scores and Credit Reports: How The System Really Works, What You Can Do (Privacy Times 2004), and co-author of a book with a chapter on credit reporting; (3) an expert witness qualified by the federal courts in Fair Credit Reporting Act litigation: (4) an expert on credit reporting who has testified before Congress on numerous occasions, including four hearings in 2003, and who has testified twice before the California legislature in regards to legislation on the use of financial data; and (5) an expert consultant to government agencies and private corporations, and (6) a member of the Consumer Advisory Council of Experian, one of the three national Credit Reporting Agencies (CRAs).

30. Since 1981, I have been Editor/Publisher of *Privacy Times*, a biweekly, Washington-based newsletter that reports on privacy and information law, including the Fair Credit Reporting Act. The newsletter ranges from 8-12 pages, 23 issues per year. This means that in this newsletter (and its three-year predecessor), I have researched, written, edited and published an estimated 2,000 pages relating to information law and policy, including Congressional and State legislative actions, judicial opinions, technology developments, industry trends and actions, executive branch policies and consumer news. By my conservative estimate, at least 20 percent of my professional work since 1977 has concerned issues relating to consumer reporting and personal financial information. These endeavors have allowed me to accumulate a specialized body of knowledge in relation to the collection, use and disclosure of credit report data and personal financial information, and the standards governing them. *Privacy Times* is a subscription-only newsletter. The readers are generally the attorneys and specialists within government agencies, corporations, law firms, universities and public interest groups that are responsible for issues relating to freedom of information and privacy laws, including the FCRA and similar State statutes.

31. I am author of the book, Credit Scores and Credit Reports: How The System Really Works, What You Can Do, 3rd Ed. (Privacy Times 2007). The book has 23 Chapters, 399 pages and 415 footnotes. As the title indicates, it describes how the credit scoring and credit reporting systems work and what consumers can do to obtain their reports, read and understand them, correct errors in them and enforce their rights. I also am co-author of Your Right To Privacy: A Basic Guide To Legal Rights In An Information Society (2nd Edition, Southern Illinois University Press, 1990), which has a chapter on credit reporting. I was also a contributor to Fair Credit Reporting, 6th Ed. (National Consumer Law Center, 2006), the leading manual for FCRA practitioners.

[5] See U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989), "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."

32. Since the early 1990s, I have served as an expert witness in numerous FCRA cases and have been qualified by the federal courts.[6] As an expert witness, I have had the opportunity to read thousands of pages of deposition testimony by consumer reporting agency officials and by credit grantor personnel responsible for reporting data to CRAs. This is significant because CRAs and credit grantors do not openly discuss or publish information on their procedures and practices for handling personal data. In fact, CRAs typically consider such procedures and practices to be proprietary and/or trade secrets. To my knowledge, the best (and possibly only) sources for finding candid descriptions of CRAs' and credit grantors' procedures and practices in relation to credit reporting data are the depositions of CRA and credit grantor employees in FCRA litigation.

33. I have testified before Congress on numerous occasions, including the Congress's only FCRA oversight hearing in 2007, held by the House Financial Services Committee, entitled, "Credit Reports: Consumers' Ability to Dispute and Change Information."[7] I also testified on four occasions in 2006 and 2005 (see attached CV).

In 2003, I testified twice before the Senate and twice before the House, including the July 10, 2003 Senate Banking Committee hearing, "The Accuracy of Credit Report Information and the Fair Credit Reporting Act;"[8] and the June 12, 2003 House Financial Services Subcommittee on Financial Institutions & Consumer Credit hearing, "The Role of FCRA in the Credit Granting Process."[9]

34. From 2002 – 2004, I served on the Consumer Advisory Council of Experian (formerly TRW), a national CRA and vendor of other information services. The Council meets twice a year to advise the company on a host of credit reporting, marketing and other privacy-related topics. Since August 1998, I have served under contract as a member of the Social Security Administration's Panel Of Privacy Experts advising the agency on a host of issues. In 2002, the U.S. Postal Service retained me under contract to review its re-writing of its Privacy Act notices to ensure they were understandable to the public and consistent with the Privacy Act's goals of ensuring FIPs. In 1990, Equifax, another national CRA, published "The Equifax Report on Consumers In the Information Age," a nationwide opinion survey and analysis by Louis Harris and Associates and Prof. Alan F. Westin. The report listed me as a privacy expert to whom the authors expressed appreciation for my advice on survey coverage.

---

[6] See, for example, Adelaide Andrews v. TRW, Inc. 225 F.3d 1063 (9th Cir. 2000). Although the trial judge qualified me, the 9th Circuit, in reversing part of her opinion in favor of defendant, ruled that she overly limited the scope of my testimony as to the prevalence of identity theft and its impact on credit report accuracy and integrity. "In making that determination the jury would be helped by expert opinion on the prevalence of identity theft, as the district court would have been helped if it had given consideration to the Plaintiff's witnesses on this point before giving summary judgment," the 9th Circuit panel wrote.

[7] www.house.gov/apps/list/hearing/financialsvcs_dem/hl061907.shtml

[8] http://banking.senate.gov/03_07hrg/071003/index.htm

[9] http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=229).

/s/ Evan D. Hendricks

Evan D. Hendricks
P.O. Box 302
Cabin John, M.D. 20818
(301) 229-7002

November 29, 2012